GESTIÓN DEL RIESGO INFORMÁTICO EN SMARTPHONE Y SU USO EN LA BANCA ELECTRÓNICA

Maldonado Casadiegos Alexander.
8529alex@gmail.com
Universidad Piloto de Colombia

Resumen—En este documento se comentan los aspectos más importantes de la gestión del riesgo informático en smartphone y las actividades que se pueden ver afectadas por no realizar una adecuada gestión en su manejo desde la perspectiva de usuarios finales. Teniendo en cuenta las mejores prácticas para asegurar la no afectación en los servicios en línea.

Abstract— This document discusses the most important aspects of the computer risk management in smartphone and the activities that can be affected by not performing an adequate management in its handling from the perspective of end users. Taking into account best practices to ensure non-involvement in online services.

Índice de Términos—Aseguramiento, banca digital, dinero digital, gestión de riesgos, antivirus, malware, plataformas móviles, troyano, ransomware, botnet, seguridad, medidas de seguridad, dispositivos móviles, smartphone.

I. INTRODUCCIÓN

En la nueva era del mundo digital se logra evidenciar como los sectores económicos y sociales están preocupados por las nuevas amenazas de dicha era y en esta preocupación se pueden resaltar las entidades bancarias las cuales han adaptado sus servicios en productos en línea para agregar un valor al consumidor y es por ello que la banca electrónica está a la vanguardia en la tecnología para lograr ampliar sus mercados y además fortalece su infraestructura tecnológica en el área de seguridad informática, la cual se ha convertido en un factor clave para evitar riegos a los consumidores y al mismo sector bancario.

El desarrollo continuo de la banca electrónica ha contribuido a mejorar la calidad del sistema bancario reduciendo aspectos importantes como: el costo y el tiempo de las transacciones que utilizan los clientes, así como asegurar que al realizar estas operaciones no se verán comprometidas información en los aspectos de confidencialidad, integridad y disponibilidad de la información que se está manejando en estos sistemas electrónicos.

El desarrollo y uso de las transacciones electrónicas se encuentran todavía en las etapas iníciales, lo cual permite incluir la tecnología y conciencia de lo importante que es realizar una adecuada gestión del riesgo informático en seguridad informática. Y por último es importante resaltar el compromiso de las autoridades que están supervisado que dichas políticas de gestión de riesgo informático sean aplicadas de manera adecuada, teniendo como objetivo no obstaculizar la innovación en la banca electrónica y las actividades con dinero electrónico.

II. BANCA DIGITAL, DINERO DIGITAL, ANTIVIRUS

Banca Digital

La banca digital es un servicio ofrecido en su mayoría por las entidades financieras que tiene como objetivo permitir a sus clientes ejecutar operaciones y transacciones monetarias con sus productos de forma autónoma, independiente, segura y rápida. Entre las transacciones más comunes que se pueden realizar a través de un servicio de banca electrónica se encuentran las transferencias, pago de facturas y la consulta de los movimientos de las cuentas entre otras muchas más opciones.

El servicio de banca electrónica se presta de la misma forma para empresas que para particulares y las empresas son las que hacen una utilización más intensiva, dinámica y profesional ya que su gestión diaria hace que eviten paseos innecesarios a la sucursal bancaria y la banca electrónica está implantada en España desde el año 1995 cuando las entidades financieras decidieron apostar por este servicio organizando y racionalizando sus sistemas

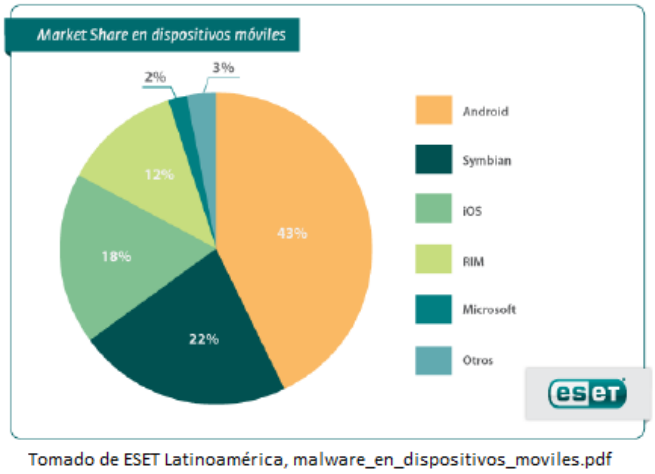
de información para construir infraestructuras que facilitaran la gestión de clientes mediante el acceso a Internet y en el momento actual se encuentra muy integrada entre todos los canales de contacto: Internet, servicio telefónico e incluso desde el móvil, [1].

Dinero Digital

Dinero digital es la representación digital de una cantidad de moneda respaldada por una cuenta bancaria y/o tarjeta de crédito que garantiza la existencia de los fondos y en la actualidad hay mucho trabajo detrás de iniciativas que buscan impulsar su uso gracias a su seguridad, economía, penetración y alcance en comparación del papel moneda tradicional. El dinero digital utiliza un teléfono móvil que sirve como billetera donde puede realizar diversas transacciones en su día a día. [2].

III. PLATAFORMAS MÓVILES

En el mundo de los dispositivos móviles existe una diversidad de plataformas las cuales están a disposición de los usuarios, caso contrario con los pc de escritorio donde aún windows posee amplia mayoría del mercado, pero al momento de adquirir un smartphone, los usuarios tienen diversidad de opciones para elegir y actualmente el mercado se encuentra dividido principalmente entre 5 sistemas operativos: android, symbian, windows mobile, ios, y rim donde cada una de estas plataformas cuenta con diferentes características en lo que respecta a sus funcionalidades, distribución de aplicaciones y modelo de seguridad dado lo anterior ha llevado a los desarrolladores de códigos maliciosos a focalizarse en las plataformas de mayor popularidad con el fin de llegar así a una mayor cantidad de víctimas y según la información publicada a mediados del 2011 por la consultora gartner el mercado de los dispositivos móviles es liderado por android con el 43% del total, seguido por symbian (22%), ios (18%), rim(12%) y windows phone en la quinta posición con el 2%: [3]



Tomado de ESET Latinoamérica, malware_en_dispositivos_moviles.pdf

Imagen 1 - Market Share de Smartphone
Fuente:ESET Latinoamérica

Android

Es la plataforma móvil de google y esta se encuentra en el mercado desde septiembre del 2008 la cual hoy en día es una de las plataformas móvil líderes en teléfonos inteligentes y como consecuencia es una de las plataformas para la cual más códigos maliciosos están apareciendo y explotando ciertas características presentes en la arquitectura del sistema y sus repositorios de aplicaciones y desde el 2011 se han aumentado amenazas para esta plataforma. El desarrollo de este sistema operativo está centrado en un núcleo basado en linux para los servicios base y este trabaja sobre capas de abstracción entre el hardware y el software, la capa que ofrece el núcleo del sistema se encuentran librerías desarrolladas en C/C++ las cuales permiten manejo de gráficos y otras funcionalidades como las bases de datos sq-lite y también se encuentra el runtime de android formado por un conjunto de bibliotecas base desarrolladas en java dónde por cada aplicación que se encuentre se ejecuta un proceso separado dentro de la máquina virtual de dalvik y los permisos necesarios para la ejecución de una aplicación se encuentran en el androidmanifest.xml, android asigna un usuario id y un grupo id distinto a cada una de ellas de esta manera cada proceso se ejecuta de manera aislada ofreciendo un modelo de seguridad compacto y eficiente por lo general el método de propagación de amenazas para esta plataforma suele ser a través de cuentas de desarrolladores falsas que publican aplicaciones maliciosas en el android market o a través de repositorios de aplicaciones no oficiales y desde mediados del 2010 se ha incrementado la cantidad de

amenazas existentes para android en dónde han aparecido diferentes códigos maliciosos como geinimi, droiddream y raden, dichos troyanos se encontraban ocultos dentro de videojuegos ocultando su verdadera identidad y comportamiento. En el caso puntal de raden, troyano sms detectado por eset mobile security la amenaza se encontraba oculta en juegos (como el conocido buscaminas) en dónde al iniciarse el mismo se ejecutaba la función (startnewgame ()) y luego de configurar todos los parámetros se realizaba el llamado a la función sendsms() que se encarga de enviar un mensaje de texto para suscribir al usuario a un servicio de mensajes Premium y la función sendsms() envía un mensaje de texto al número 1066185829 con el contenido 921X2 suscribiendo al equipo infectado a un servicio de mensajería premium y para ocultar su comportamiento esta amenaza captura los mensajes de respuesta del servicio de mensajes y evita su notificación al usuario para evitar ser detectado y otras amenazas como las mencionadas anteriormente permiten la recepción de comandos remotos haciendo que el dispositivo se convierta en un equipo zombi perteneciente a una botnet, en estos casos el botmaster puede efectuar comandos para acceder a información personal del usuario o instalar otros códigos maliciosos en el equipo y android es una plataforma relativamente nueva no obstante ha sido víctima de códigos maliciosos innovadores y avanzados que utilizan las funcionalidades del sistema operativo de google para beneficio de los desarrolladores de códigos maliciosos y a lo largo del 2011 el laboratorio de análisis e investigación de eset latinoamérica se analizó 41 familias de códigos maliciosos de las cuales 15 eran troyanos sms, esto posiciona a los troyanos sms como una de las técnicas más utilizadas por los desarrolladores de malware además el 65% de las amenazas aparecen en los últimos cinco meses destacando la tendencia identificada por el laboratorio de eset para el 2012. También existen falsas soluciones de seguridad que engañaban al usuario bajo la promesa de proteger el smartphone cuando en realidad robaban información personal y otras conclusiones de este análisis que realizó el laboratorio de eset latinoamérica son:

• El 30% de las amenazas estuvieron disponibles para su descarga en el android market.

• El 37% son troyanos sms.

• El 60% de los códigos maliciosos tiene alguna característica de botnets es decir, algún tipo de control remoto sobre el dispositivo. [3]

Tomado de ESET Latinoamérica, malware_en_dispositivos_moviles.pdf

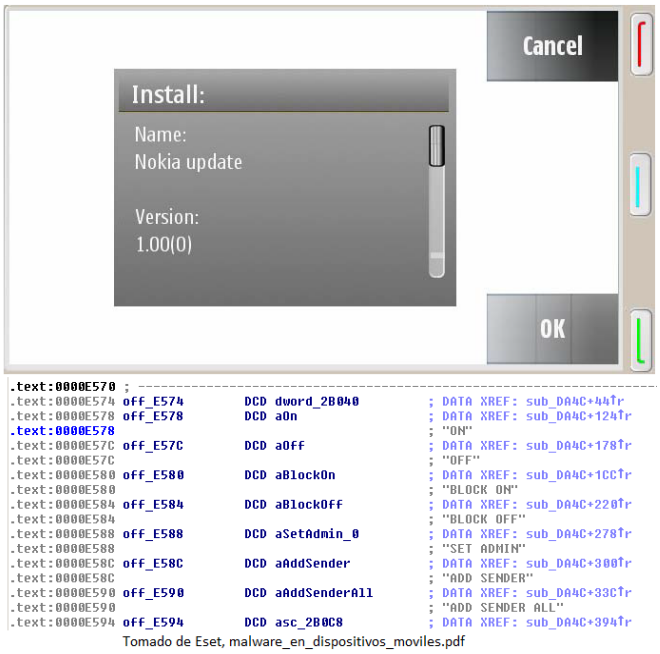
Imagen 2 - Inicio de Juego

Fuente:ESET Latinoamérica

Symbian

Está en el mercado desde hace más de una década y este ha sido por mucho tiempo una de las plataformas móviles de mayor uso a nivel mundial y a lo largo de su historia y con la evolución de su sistema operativo surgieron distintas amenazas que intentaron burlar el modelo de seguridad, este sistema operativo centra su arquitectura de seguridad en dos conceptos: data caging y capabilities, en donde cada aplicación solo cuenta con acceso a sus recursos o determinadas áreas del sistema de archivos y de esta forma se evita que una aplicación pueda acceder al directorio privado de otra o a los datos y existen distintos tipos de accesos dentro del

sistema de archivos con funciones específicas: /resources: se permite la escritura en el momento de la instalación de una aplicación, la lectura de su contenido no se encuentra restringida y contiene los íconos de las aplicaciones, mapas de bits, etc /sys: almacena los archivos binarios, los registros de instalación y los certificados de administradores (root) y su escritura está permitida durante la instalación de las aplicaciones y la lectura solo para backups /private: sección privada designada para cada aplicación en donde se puede almacenar la información privada /all the rest: documentos compartidos que pueden ser accedidos por todas las aplicaciones y servicios del sistema como por ejemplo fotografías, música y documentos, las aplicaciones para esta plataforma cuentan con una firma digital que garantiza su veracidad, actualmente existen distintos tipos de certificados para aplicaciones y según los recursos a los que solicita acceso y también este certificado puede ser falsificado por algunas amenazas y esta es una de las maneras utilizadas para engañar al usuario e infectar su dispositivo y para Symbian los códigos maliciosos pueden propagarse en archivos con extensión sis o también ser desarrollados en java ya que la plataforma soporta cualquier formato y estas amenazas cuentan con capacidades que van desde el envío de mensajes de texto a números premium y hasta el robo de credenciales bancarias los troyanos bancarios para plataformas móviles han evolucionado con el pasar de los años y una de las amenazas para symbian fue zitmo, un troyano que convertía el dispositivo en una botnet dedicada al robo de credenciales bancarias. Zitmo significa "zeus in the mobile" y es una variante del popular crimepack zeus para dispositivos móviles y la propagación de este troyano es a través de mensajes de texto los cuales simula ser un certificado que le permite al usuario acceder a información de la banca electrónica y el número de la posible víctima es obtenido a través de una computadora infectada con zeus que como parte del engaño invita al usuario a ingresar la información de su celular: marca y modelo y plataforma del mismo y con esta información el atacante envía un mensaje que contiene el enlace a la descarga de zitmo según los datos ingresados por el usuario y cuando el usuario selecciona el enlace, descarga lo que supone ser una actualización de seguridad, pero no es más ni menos que el troyano y las características más importantes de zitmo son: éste puede ser administrado de manera remota y envía la información a un número de teléfono almacenado como admin y permiten especificar qué información será redirigida al atacante, desactivar o activar la captura de mensajes y modificar la lista de contactos y estos son los principales comandos conocidos: block on: ignorar todos los comandos block off: habilitar los comandos remotos, set admin: cambiar el número del centro de control, sender add: agregar un contacto, sender rem: eliminar un contacto, set sender: actualizar un contacto [3]



Tomado de Eset, malware_en_dispositivos_moviles.pdf

Imagen 3 - Zitmo, supuesta actualización

Fuente:ESET Latinoamérica

Windows Mobile

Microsoft tiene su plataforma para dispositivos móviles ya hace algunos años y en sus primeras versiones eran llamadas como pocket pc y las más actuales que han introducido distintos cambios en lo que respecta a arquitectura, funcionalidades y seguridad y en relación a su seguridad, windows mobile utiliza una combinación de políticas de seguridad, roles y certificados para gestionar la ejecución de aplicaciones en el sistema, es decir, la estructura es muy similar a la del sistema operativo windows para computadoras de escritorio o notebook. Las políticas de seguridad permiten

configurar si una aplicación o instalación se puede ejecutar o debe ser bloqueada permitiendo solo la instalación y ejecución de aplicaciones firmadas y en algunos casos pregunta al usuario antes de efectuar cualquier acción.

En lo que respecta a permisos de ejecución de aplicaciones existen: con privilegios, normal, bloqueado y una aplicación que se ejecute con privilegios podrá realizar cambios a nivel de configuración lo que podría resultar malo para el sistema ya que cuenta con permisos de acceso completo a archivos del sistema.

Las aplicaciones en windows mobile suelen ejecutarse en modo normal ya que de esta manera se restringe la llamada a ciertas api y cuando una aplicación se ejecuta con este nivel de permisos puede leer pero no escribir en zonas protegidas del registro y archivos del sistema y el directorio \windows\system. [3]

IOS

Apple diseño ios, el cual es su sistema operativo para plataformas móviles; que incluye al iphone, iPad e ipod y actualmente la última versión de disponible es ios 10 desarrollado íntegramente en el lenguaje objetive-c, c y c++.

Este sistema operativo fue publicado en el 2007 durante la macworld conference & expo en conjunto con el iphone y desde ese entonces se han publicado nuevas actualizaciones que incluyeron entre otras cosas la posibilidad de ejecutar procesos de forma simultánea (multitasking) y en lo que respecta al modelo de seguridad del sistema operativo y las aplicaciones disponibles para esta plataforma apple analiza cada una de las aplicaciones antes de que se encuentren disponibles. [3][4]

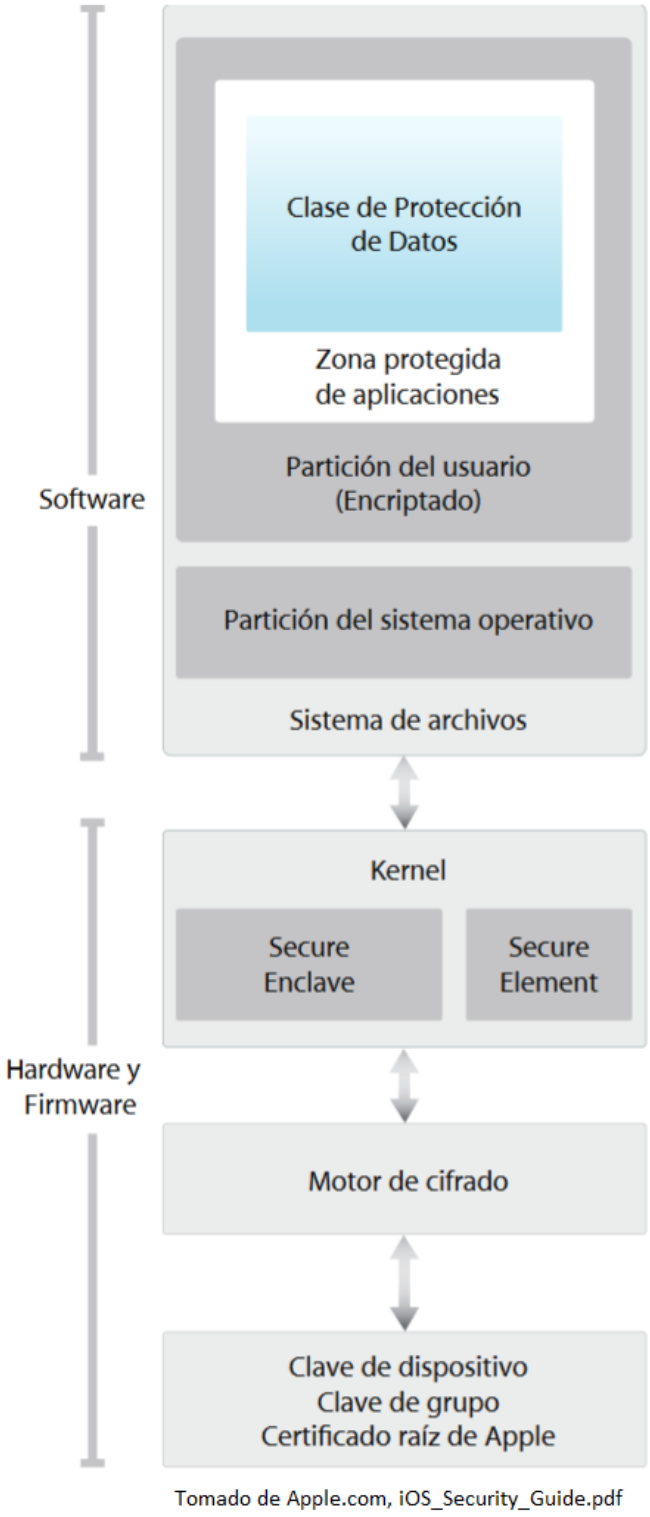


Imagen 4 - Diagrama de la arquitectura de seguridad de iOS
Fuente:ESET Latinoamérica

BlackBerry

Diseñado y creado por research in motion (rim), blackberry se encuentra en el mercado desde 1999 y es era una de las plataformas preferidas por el sector empresarial esta preferencia se debía principalmente a que soportaba correo electrónico corporativo a

través de midp(mobile information device profile), funcionalidad que permite interacción con microsoft exchange, lotus dominio o novell y para el desarrollo de aplicaciones para estos dispositivos se encuentran las api de esta plataforma y a modo de seguridad para la utilización de ciertas funcionalidades, las mismas deben estar firmadas digitalmente. El núcleo del sistema operativo está basado en c++, aunque el desarrollo de las aplicaciones se realiza en Java. [3]

IV. MALWARE EN DISPOSITIVOS MÓVILES

Muchos usuarios de los dispositivos de Smartphone desconocen que las plataformas móviles son utilizadas por los desarrolladores de códigos maliciosos para enviar enlaces dañinos que redirigen al usuario a la descarga de malware, y es debido a ello que caen víctimas de los engaños y la falta de conocimiento acerca de las amenazas para dispositivos móviles y expone a los usuarios a la pérdida de su información o la infección de su Smartphone. [3].Los troyanos en los smartphone más peligrosos del 2016 fueron los malware de tipo publicitarios con derechos de súper-usuario y estos corresponden a Trojan.AndroidOS.Ztorg y Trojan.AndroidOS.Iop y estos códigos maliciosos crecieron a lo largo de 2016 y duplicando su presencia en el top 30 de troyanos más populares en relación con el año 2015 y para conseguir derechos de súper-usuario deben usar diferentes exploits o los derechos de súper-usuario existentes si el dispositivo ya estaba rooteado. [5]

IV. GESTIÓN DE RIESGOS: "LA EDUCACIÓN EN SEGURIDAD, UNA RESPONSABILDIAD SOCIA"

Muchos usuarios del internet se han encontrado con la amenaza de la nombrada estafa nigeriana pero a pesar de que esta se puede identificar fácilmente, la realidad es que todavía hay personas que cae en este engaño, unas por inocentes y desconocedoras y otras porque por simple curiosidad contestan para ver qué va a pasar y como resultado caen en la trampa y la "estafa nigeriana" o "estafa 419" tiene origen en el siglo XIX y probablemente desde antes y era con cartas ofreciendo distribuir un jugoso tesoro pero esta estafa centenaria lejos de desaparecer se volvió a tomar fuerza con la evolución de la tecnología y con el tiempo aparecieron múltiples versiones que migraron al correo electrónico y luego de tanto tiempo aún se siguen recibiendo mensajes en redes sociales y páginas web con el mismo tipo de engaño o estafa como por ejemplo: eres el visitante número 1.000.000 te ganaste una lotería fuiste elegido para un viaje pero si las amenazas informáticas han venido evolucionando en los últimos años y ya hasta hablamos de ataques dirigidos, ciberguerra y apt ¿Por qué aún se ven este tipo de engaños? en los últimos años, los riesgos han ido evolucionando tales como ciberespionaje, ataques dirigidos, amenaza a la privacidad y retos de seguridad en los nuevos dispositivos IoT y el no menos maléfico el ransomware y el cual a aumentando su cantidad de víctimas y sin embargo las amenazas anteriores tienen un factor en común: "el usuario" y bien sea por un correo electrónico, un dispositivo USB abandonado apropósito en un sitio público o un mensaje en una red social o una contraseña débil. Los atacantes encuentran que los usuarios presentan un comportamiento inocente y en muchos casos irresponsable al comprometer la seguridad de un sistema como los son sus dispositivos móviles y lamentablemente esta realidad seguirá siendo la que aprovechada por los atacantes y a pesar de que puedan existir vulnerabilidades en dispositivos o aplicaciones que le permitan a un atacante tomar el control de un sistema y la forma más sencilla de hacerlo será a través del engaño a los usuarios ¿por qué habría de gastar horas en desarrollar un exploit cuando con un simple correo electrónico se puede lograr el mismo tipo de acceso a los sistemas? o ¿por qué un ladrón se tomaría el esfuerzo de cavar un túnel para entrar a una casa si solo tiene que llamar a la puerta? El cibercrimen es una actividad al margen de la ley pero eficiente es decir, es difícil negar que las evoluciones de las familias de códigos maliciosos como el ransomware seguirá gobernando como la amenaza con mayor crecimiento y que de a poco se verán más amenazas para dispositivos móviles y el cibercrimen ha llegado a nombrarse como una actividad despiadada donde sectores como el de la salud se ven amenazado e infraestructuras como las de los cajeros automáticos están en un riesgo a nivel mundial y desde el año inmediatamente anterior se ha logrado evidenciar cómo los cibercriminales van evolucionando no solo con diferentes tipos de

software malicioso y técnicas de ingeniería social sino también con "planes de negocio" para extorsionar a sus víctimas y obtener algún tipo de ganancia económica.

Estamos frente a la necesidad de dejar de hablar genéricamente sobre los riesgos de seguridad y es necesario que los usuarios y/o personas del común reconozcan que pueden verse afectados y que desde un fraude por correo electrónico hasta un secuestro de información y todos deben verse como factibles y que es necesario tomar las medidas de concientización y tecnológicas para evitarlos y la educación no es solo cuestión de edad el mundo actual es un mundo digital que está habitado por dos tipos de factores: los nativos digitales y los inmigrantes digitales. Los nativos digitales tienen incorporado el uso de la tecnología en la mayoría de los aspectos de su vida diaria desde temprana edad y en cambio los inmigrantes digitales la usan para resolver muchas de sus actividades diarias a pesar de que tuvieron que adaptarse y acostumbrarse a hacerlo y sería lógico de esperar que los nativos digitales sean menos susceptibles a este tipo de engaños y sin embargo, un estudio del BBB Institute dejó en evidencia que los jóvenes de entre 25 y 34 años son más susceptibles a scams, mientras que otros estudios demuestran que los más jóvenes son los que tienen los comportamientos más riesgosos al momento de navegar en internet tales como conectarse a redes wi-fi poco seguras, conectar dispositivos USB que les dan terceros sin mayores cuidados y la poca utilización de soluciones de seguridad. y los inmigrantes digitales pueden ser más cautelosos al momento de utilizar la tecnología, nos encontramos con que muchas veces pueden ser víctimas de ataques o tener comportamientos poco seguros y generalmente se debe al desconocimiento de las características de seguridad que pueden tener los diferentes dispositivos o a la falta de información sobre el alcance de las amenazas informáticas y el cuidado que se debería tener. En conclusión no importa la edad y la necesidad real es que todos los usuarios conozcan sobre las amenazas la forma de cómo es que actúan y las mejores alternativas para proteger sus dispositivos móviles. Son características en los cuales los usuarios deben enfocarse para protegerse y la paradoja actual: más información, menos sensación de seguridad sin lugar a dudas hace ya casi cuatro años después de las revelaciones de Snowden la sensación de seguridad en relación a la información es cada vez menor y lo paradójico es que en la actualidad hay más información acerca de lo que pasa con ella y una de las lecciones más importantes que se debería haber aprendido a partir de las revelaciones de Snowden es si se autoriza a alguien a actuar en secreto y se le adjudica un presupuesto considerable no se puede suponer que por más que sea buena persona va a hacer lo correcto, de la forma correcta y sin consecuencias perjudiciales y lo importante que lo anterior no se trata de volverse paranoico o en no querer tener ningún tipo de conexión en internet y como reto importante a enfrentar es la necesidad de educarse acerca de cómo protegerse en la red qué tipo de información publicar y cuáles son las medidas de protección que van a permitir garantizar la seguridad y privacidad de la información, los pequeños cambios hacen grandes diferencias y la seguridad informática no se trata solamente de una solución tecnológica ya que también hay un componente humano que es necesario proteger y los esfuerzos de concientización en seguridad informática ya son una realidad en muchos ámbitos de la vida actual, hay muchos usuarios que aún no cuentan con una formación adecuada en estos temas y aunque muchos reconocen las amenazas para computadoras aún no las reconocen en los dispositivos móviles y de acuerdo a encuestas realizadas por este, solamente el 30% de los usuarios utiliza una solución de seguridad en sus dispositivos móviles a pesar de que más del 80% reconoce que los usuarios son los que tienen la mayor cuota de responsabilidad al momento de caer en engaños por no tomar consciencia ni educarse sobre las diferentes estafas. Así que es necesario que se piense en la seguridad en todo momento y contexto desde un dispositivo de uso personal con conexión wi-fi hasta infraestructuras críticas conectadas y manipuladas de forma remota a través de internet y es una realidad que todas las tecnologías cambian rápidamente y cada vez hay más modos de infección, que pueden ser fácilmente aprovechados por los atacantes si los usuarios no están educados en estos temas. Importante resaltar que no se puede permitir que el avance de la tecnología se vuelva en contra del usuario. [6]

VI. CONCLUSIONES

La banca digital busca ofrecer facilidades en utilizar los servicios financieros en los diferentes dispositivos móviles y que para ofrecer este servicio las entidades bancarias han robustecido su infraestructura tecnológica para evitar posibles fraudes y estafas.

La gestión del riesgo para el servicio de banca digital utilizando los Smartphone se deben tratar desde los usuarios finales, ya que en la mayoría de los casos es mucho más fácil lograr objetivo fraude desde estos que un ataque a los diferentes servicios que ofrecen las entidades financieras y las entidades financieras deben contar con un plan de concienciación para el público en general con el fin de que logren mitigar y minimizar los fraudes que se presentan en la Banca Electrónica.

REFERENCIAS

[1] La banca electrónica es un servicio para empresas y autónomos disponible en: http://blog.sage.es/innovacion-tecnologia/la-banca-electronica-es-un-servicio-para-empresas-y-autonomos/.

[2] Qué es dinero digital disponible en: http://blog.soyfri.com/2016/11/21/que-es-dinero-digital/

[3] Malware en dispositivos móviles disponible en: http://www.welivesecurity.com/wp-content/uploads/2014/01/malware_en_dispositivos_moviles.pdf.

[4] iOS Security Guide disponible en: https://www.apple.com/es/business/docs/iOS_Security_Guide.pdf

[5] Kaspersky Security Bulletin 2016 Review SP disponible en: https://kasperskycontenthub.com/securelist-spain/files/2016/12/Kaspersky_Security_Bulletin_2016_Review_SP.pdf.

[6] Tendencias2017-eset disponible en: http://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf.

[7] Circular 042 de 2012 Superintendencia Financiera de Colombia disponible en: http://www.certicamara.com/download/correspondencia/20121005_Anexos_12_circular_042_de_2012.pdf.